Repository and Client Wish List

Noel Nazario, NIST

for

Federal PKI TWG

Scope and Purpose

- Existing repository and client implementations provide uneven level of service
- The purpose is to identify functionality necessary to support the Federal PKI
- This document should focus on minimum requirements for interoperability and uniform level of service.

Repository Functional Areas

- Access protocol (queries)
- Management protocol (updates)
- Management functions
- Inter-repository functions
- Schema definition
- Performance and Scalability
- Security

Protocols

- Access (queries)
  - LDAP v2, LDAP v3, DAP, Other
  - Authentication (none, password, certificate-based)
- Management
  - LDAP v2, LDAP v3, DAP, Other
  - Authentication (password, certificate-based)

Management Functions

- Mostly out of scope for interoperability except for name-space management, backup, and archive requirements.
- Support for management roles and separation of duties may be desirable.

Inter-Repository Functions

- Chaining - local repository communicates transparently with appropriate repository to respond to a query
- Shadowing - information maintained by a remote repository is replicated locally
- Referrals - repository responds a failed query with the name of a repository that could have the information requested

Schema Definitions

- Schema - The data objects included in each data entry or record
- Minimum set of data objects required by FPKI should be identified (e.g., Certificate, Cross-Certificate, CRL)
- Objects not required by FPKI should be left out, but not restricted.

Performance and Scalability

- Can agreement be obtained on what is acceptable performance or should it be left to implementors?
- Should minimum requirements be imposed on scalability? Can/Should guidance be offered?

Security

- Access control
- Authentication
- Audit logs
- Roles and separation of privileges
- Denial of service attack protection (mostly external measures)
- Redundancy and other physical protections (external measures)

Client Functional Areas

- Access protocols (queries)
- Authentication
- User interface
- Certificate chain handling

Client Specific Issues

- Topics are similar to repository, although mechanisms may differ.
- Referral support would require smarter client than dependence on chaining.
- Need to process certificate chains and verifications as transparently as possible.
- Other

What's Next?

- First draft due next meeting.
- Set level of detail
- Take a shot at setting priorities.
- Should we be more/less X500 specific?
- What's the status of other approaches?
- Discussion and other inputs are needed (suggestions/text).